

**Федеральное государственное автономное образовательное
учреждение высшего образования
«Московский физико-технический институт
(национальный исследовательский университет)»**

УТВЕРЖДЕНО

**Директор физтех-школы
прикладной математики и
информатики**

А.М. Райгородский

	Рабочая программа дисциплины (модуля)
по дисциплине:	Криптографические протоколы
по направлению:	Информатика и вычислительная техника
профиль подготовки:	Физтех-школа Прикладной Математики и Информатики кафедра дискретной математики
курс:	4
квалификация:	бакалавр

Семестр, формы промежуточной аттестации: 7 (осенний) - Дифференцированный зачет

Аудиторных часов: 30 всего, в том числе:

лекции: 15 час.

семинары: 15 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 15 час.

Всего часов: 45, всего зач. ед.: 1

Количество контрольных работ, заданий: 1

Программу составил: Д.В. Мусатов, канд. физ.-мат. наук, доцент

Программа обсуждена на заседании кафедры дискретной математики 05.03.2020

Аннотация

Курс посвящен изучению основных понятий математической криптографии, методам синтеза и анализа криптографических протоколов, протоколам аутентификации. В курсе рассматриваются функции криптографических протоколов, их классификация, основные задачи. Кроме того, в курсе рассматриваются разновидности атак на протоколы и требования к безопасности протокола.

1. Цели и задачи

Цель дисциплины

ознакомление студентов с основными понятиями математической криптографии, методами синтеза и анализа криптографических протоколов, протоколами аутентификации.

Задачи дисциплины

- освоение студентами базовых знаний (понятий, концепций, методов и моделей) в области криптографии;
- выработка навыка практического использования соответствующих технологий.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 Анализирует задачу, выделяя этапы ее решения, действия по решению задачи
	УК-1.2 Находит, критически анализирует и выбирает информацию, необходимую для решения поставленной задачи
	УК-1.3 Рассматривает различные варианты решения задачи, оценивает их преимущества и недостатки
	УК-1.4 Грамотно, логично, аргументированно формирует собственные суждения и оценки
	УК-1.5 Определяет и оценивает практические последствия возможных вариантов решения задачи
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1 Формулирует совокупность взаимосвязанных задач в рамках поставленной цели работы, обеспечивающих ее достижение. Определяет ожидаемые результаты решения поставленных задач
	УК-2.2 Проектирует решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений
ОПК-4 Способен осуществлять сбор и обработку научно-технической и (или) технологической информации для решения фундаментальных и прикладных задач	ОПК-4.1 Владеет методами научного поиска и интеллектуального анализа информации при решении задач профессиональной деятельности
	ОПК-4.2 Знает основные источники научно-технической и (или) технологической информации в области профессиональной деятельности
	ОПК-4.3 Умеет составлять аннотации, рефераты, библиографические перечни и обзоры информации в области своей профессиональной деятельности
	ОПК-4.4 Владеет навыками работы с компьютером и компьютерными сетями с целью получения, хранения и обработки научной (технической, технологической) информации
ОПК-5 Способен участвовать в проведении фундаментальных и прикладных	ОПК-5.1 Способен решать поставленные задачи в области теоретических и экспериментальных исследований и разработок

исследований и разработок, самостоятельно осваивать новые теоретические, в том числе, математические методы исследований и работать на современной экспериментальной научно-исследовательской, измерительно-аналитической и технологической аппаратуре)	ОПК-5.2 Обладает способностью к освоению новых знаний на основе изучения литературы, научных статей и других источников
	ОПК-5.3 Способен к профессиональной эксплуатации современной экспериментальной научно-исследовательской (измерительно-аналитической и технологической) аппаратуры
ПК-1 Способен ставить, формализовывать и решать задачи, в том числе разрабатывать и исследовать математические модели изучаемых явлений и процессов, системно анализировать научные проблемы, получать новые научные результаты	ПК-1.2 Способен выдвигать гипотезы, строить математические модели для описания изучаемых явлений и процессов, оценить качество разработанной модели
	ПК-1.1 Способен находить, анализировать и обобщать информацию об актуальных результатах исследований в рамках тематической области своей профессиональной деятельности
	ПК-1.3 Способен применять теоретические и (или) экспериментальные методы исследований к конкретной научной задаче и интерпретировать полученные результаты
ПК-2 Способен самостоятельно или в качестве члена (руководителя) малого коллектива организовывать и проводить научные исследования и их апробацию	ПК-2.1 Знает принципы построения научной работы, методы сбора и анализа полученного материала, способы аргументации
	ПК-2.2 Способен планировать и проводить научные исследования самостоятельно или в качестве члена (руководителя) малого научного коллектива
	ПК-2.3 Способен проводить апробацию результатов научно-исследовательской работы посредством публикации научных статей и участия в конференциях

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- основные понятия, законы, теории части криптографии;
- современные проблемы соответствующих разделов криптографии;
- современные подходы и методы для решения типовых прикладных задач криптографии.

уметь:

- понять поставленную задачу;
- использовать свои знания для решения и прикладных задач криптографии;
- самостоятельно находить алгоритмы решения задач, в том числе и нестандартных, и проводить их анализ;
- самостоятельно видеть следствия полученных результатов.

владеть:

- навыками освоения большого объема информации и решения задач (в том числе, сложных);
- навыками самостоятельной работы и освоения новых дисциплин;
- культурой постановки, анализа и решения прикладных задач криптографии.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост.

		лекции	семинары	лаборат. работы	работа
1	Основные понятия и методы математической криптографии	3	3		3
2	Протоколы аутентификации	3	3		3
3	Протоколы передачи и согласования ключа	3	3		3
4	Протокол SSL/TLS	3	3		3
5	Криптографические токены	3	3		3
Итого часов		15	15		15
Подготовка к экзамену		0 час.			
Общая трудоёмкость		45 час., 1 зач.ед.			

4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 7 (Осенний)

1. Основные понятия и методы математической криптографии

Односторонняя функция, генератор псевдослучайных чисел, криптосистема с секретным ключом, криптосистема с открытым ключом, схема электронной подписи, доказательство с нулевым разглашением. Методы синтеза и анализа криптографических протоколов: классы моделей нарушителя, подходы к строгому теоретическому обоснованию стойкости, связь теоретически обоснованной стойкости и практической стойкости.

2. Протоколы аутентификации

Определения, свойства, модели нарушителя. Простейшие протоколы аутентификации в коммуникационных сетях и в встроенных системах, их уязвимости. Общие свойства протоколов аутентификации и распределения ключей: понятия явной и неявной аутентификации данных, аутентификации сущностей, подтверждения ключа. Протоколы аутентификации распределения ключа на основе криптографии с секретным ключом. Уязвимости и особенности безопасного применения данных протоколов при использовании третьей стороны. Протоколы Нидхема-Шрёдера (симметричный), Отвея-Рииса, протокол Kerberos.

3. Протоколы передачи и согласования ключа

Протоколы передачи ключа на основе криптографии с открытым ключом. Протоколы Нидхема-Шрёдера (асимметричный), X.509. Проблема повышенной вычислительной сложности и подходы к ее решению, протокол Беллера-Якоби. Протоколы согласования ключа: определения, свойства, модели нарушителя. Протоколы Диффи-Хеллмана и протоколы аутентифицированного согласования ключа на его основе: протоколы MTI/A0, STS, протокол Гюнтера. Протоколы семейства IPsec: структура, транспортный и туннельный режимы, используемые методы аутентификации и защиты данных.

4. Протокол SSL/TLS

Структура, рассматриваемые модели нарушителя, методы крипто анализа фазы передачи данных протокола TLS: методы Барда, Воденя и их развитие. Методы криптоанализа фазы согласования протокола TLS. Ошибки в использовании протокола TLS протоколами прикладного уровня: методы анализа на режим renegotiation протокола TLS.

5. Криптографические токены

Область применимости, модели нарушителя, протоколы защиты данных, требования к реализации алгоритмов. Протоколы аутентифицированной выработки ключа на основе парольной информации. Специфика моделей нарушителя при малоэнтропийном секретном элементе. Протокол ЕКЕ.

5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

учебная аудитория, оснащенная медиапроектором и экраном.

6. Перечень рекомендуемой литературы

Основная литература

1. Криптография [Текст] / Н. Смарт ; пер. с англ. С. А. Кулешова ; под ред. С. К. Ландо .— М. : Техносфера, 2006 .— 528 с.
2. Введение в криптографию [Текст] : [учеб. пособие для вузов] / под ред. В. В. Яценко .— 4-е изд., доп. — М. : МЦНМО, 2012 .— 348 с.

Дополнительная литература

1. Основы криптографии [Текст] : учеб. пособие для вузов / А. П. Алферов [и др.] .— 3-е изд., испр. и доп. — М. : Гелиос АРВ, 2005 .— 480 с.

7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

1. Сайт Технического комитета «Криптографическая защита информации» (ТК 26), <http://www.tc26.ru>.
2. Блог ООО «КРИПТО-ПРО», <http://www.cryptopro.ru/blog>.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)

учебная аудитория, экран и проектор.

9. Методические указания для обучающихся по освоению дисциплины (модуля)

1. Рекомендуется успешно сдавать контрольные работы, так как это упрощает итоговую аттестацию по предмету.
2. Для подготовки к итоговой аттестации по предмету лучше всего пользоваться материалами лекций.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению: Информатика и вычислительная техника

профиль подготовки: Физтех-школа Прикладной Математики и Информатики
кафедра дискретной математики

курс: 4

квалификация: бакалавр

Семестр, формы промежуточной аттестации: 7 (осенний) - Дифференцированный зачет

Разработчик: Д.В. Мусатов, канд. физ.-мат. наук, доцент

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 Анализирует задачу, выделяя этапы ее решения, действия по решению задачи
	УК-1.2 Находит, критически анализирует и выбирает информацию, необходимую для решения поставленной задачи
	УК-1.3 Рассматривает различные варианты решения задачи, оценивает их преимущества и недостатки
	УК-1.4 Грамотно, логично, аргументированно формирует собственные суждения и оценки
	УК-1.5 Определяет и оценивает практические последствия возможных вариантов решения задачи
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1 Формулирует совокупность взаимосвязанных задач в рамках поставленной цели работы, обеспечивающих ее достижение. Определяет ожидаемые результаты решения поставленных задач
	УК-2.2 Проектирует решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений
ОПК-4 Способен осуществлять сбор и обработку научно-технической и (или) технологической информации для решения фундаментальных и прикладных задач	ОПК-4.1 Владеет методами научного поиска и интеллектуального анализа информации при решении задач профессиональной деятельности
	ОПК-4.2 Знает основные источники научно-технической и (или) технологической информации в области профессиональной деятельности
	ОПК-4.3 Умеет составлять аннотации, рефераты, библиографические перечни и обзоры информации в области своей профессиональной деятельности
	ОПК-4.4 Владеет навыками работы с компьютером и компьютерными сетями с целью получения, хранения и обработки научной (технической, технологической) информации
ОПК-5 Способен участвовать в проведении фундаментальных и прикладных исследований и разработок, самостоятельно осваивать новые теоретические, в том числе, математические методы исследований и работать на современной экспериментальной научно-исследовательской, измерительно-аналитической и технологической аппаратуре)	ОПК-5.1 Способен решать поставленные задачи в области теоретических и экспериментальных исследований и разработок
	ОПК-5.2 Обладает способностью к освоению новых знаний на основе изучения литературы, научных статей и других источников
	ОПК-5.3 Способен к профессиональной эксплуатации современной экспериментальной научно-исследовательской (измерительно-аналитической и технологической) аппаратуры
ПК-1 Способен ставить, формализовывать и решать задачи, в том числе разрабатывать и исследовать математические модели изучаемых явлений и процессов, системно анализировать научные проблемы, получать новые научные результаты	ПК-1.2 Способен выдвигать гипотезы, строить математические модели для описания изучаемых явлений и процессов, оценить качество разработанной модели
	ПК-1.1 Способен находить, анализировать и обобщать информацию об актуальных результатах исследований в рамках тематической области своей профессиональной деятельности
	ПК-1.3 Способен применять теоретические и (или) экспериментальные методы исследований к конкретной научной задаче и интерпретировать полученные результаты

ПК-2 Способен самостоятельно или в качестве члена (руководителя) малого коллектива организовывать и проводить научные исследования и их апробацию	ПК-2.1 Знает принципы построения научной работы, методы сбора и анализа полученного материала, способы аргументации
	ПК-2.2 Способен планировать и проводить научные исследования самостоятельно или в качестве члена (руководителя) малого научного коллектива
	ПК-2.3 Способен проводить апробацию результатов научно-исследовательской работы посредством публикации научных статей и участия в конференциях

2. Показатели оценивания компетенций

В результате изучения дисциплины «Криптографические протоколы» обучающийся должен:

знать:

- основные понятия, законы, теории части криптографии;
- современные проблемы соответствующих разделов криптографии;
- современные подходы и методы для решения типовых прикладных задач криптографии.

уметь:

- понять поставленную задачу;
- использовать свои знания для решения и прикладных задач криптографии;
- самостоятельно находить алгоритмы решения задач, в том числе и нестандартных, и проводить их анализ;
- самостоятельно видеть следствия полученных результатов.

владеть:

- навыками освоения большого объема информации и решения задач (в том числе, сложных);
- навыками самостоятельной работы и освоения новых дисциплин;
- культурой постановки, анализа и решения прикладных задач криптографии.

3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

Примеры типовых контрольных заданий:

1. Методы синтеза и анализа криптографических протоколов: классы моделей нарушителя, подходы к строгому теоретическому обоснованию стойкости, связь теоретически обоснованной стойкости и практической стойкости.
2. Общие свойства протоколов аутентификации и распределения ключей: понятия явной и неявной аутентификации данных, аутентификации сущностей, подтверждения ключа.
3. Протоколы аутентификации распределения ключа на основе криптографии с секретным ключом.
4. Уязвимости и особенности безопасного применения данных протоколов при использовании третьей стороны.
5. Протоколы согласования ключа: определения, свойства, модели нарушителя.
6. Протоколы Диффи-Хеллмана и протоколы аутентифицированного согласования ключа на его основе: протоколы MTI/A0, STS, протокол Гюнтера.
7. Протоколы семейства IPsec: структура, транспортный и туннельный режимы, используемые методы аутентификации и защиты данных.
8. Протоколы аутентифицированной выработки ключа на основе парольной информации.
9. Специфика моделей нарушителя при малоэнтропийном секретном элементе.
10. Протокол ЕКЕ.

4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

1. Основные понятия математической криптографии. Односторонняя функция, генератор псевдослучайных чисел, криптосистема с секретным ключом, криптосистема с открытым ключом, схема электронной подписи, доказательство с нулевым разглашением.

2. Протоколы аутентификации. Определения, свойства, модели нарушителя. Простейшие протоколы аутентификации в коммуникационных сетях и в встроенных системах, их уязвимости.
3. Протоколы Нидхема-Шрёдера (симметричный), Отвея-Рииса, протокол Kerberos.
4. Протоколы передачи и согласования ключа. Протоколы передачи ключа на основе криптографии с открытым ключом.
5. Протоколы Нидхема-Шрёдера (асимметричный), X.509. Проблема повышенной вычислительной сложности и подходы к ее решению, протокол Беллера-Якоби.
6. Протокол SSL/TLS. Структура, рассматриваемые модели нарушителя, методы крипто анализа фазы передачи данных протокола TLS: методы Барда, Воденя и их развитие.
7. Методы криптоанализа фазы согласования протокола TLS. Ошибки в использовании протокола TLS протоколами прикладного уровня: методы анализа на режим renegotiation протокола TLS.
8. Криптографические токены. Область применимости, модели нарушителя, протоколы защиты данных, требования к реализации алгоритмов.

Критерии оценивания

- оценка «отлично (10)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений;
- оценка «отлично (9)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений;
- оценка «отлично (8)» выставляется студенту, показавшему всесторонние систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, и правильное обоснование принятых решений;
- оценка «хорошо (7)» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «хорошо (6)» выставляется студенту, если он знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «хорошо (5)» выставляется студенту, если он знает материал, и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «удовлетворительно (4)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;
- оценка «удовлетворительно (3)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет фрагментарно основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;
- оценка «неудовлетворительно (2)» выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач
- оценка «неудовлетворительно (1)» выставляется студенту, который не знает формулировок основных понятий дисциплины.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Во время проведения дифференцированного зачета обучающиеся могут пользоваться программой дисциплины.